PSEUDOCHARACTERS AND THE LENGTH BOUND

Prerequisites. Complete local noetherian rings and Hensel's lemma; the Artin–Rees lemma [AM, Cor. 10.10]; lengths of modules. From Chapter 27, *Odd Tate twists*: the groups $G_{\mathbb{Q},p}$, G_p, $\mathrm{Sha}_p(\mathbb{Q}, e)$, Problem 27.1.1 and Theorem 27.1.2. From Chapter 30, *Eisenstein congruences and Selmer classes*: Problem 30.1.1, the congruence (1), the lattices of Section 30.2 (Problems 30.2.1–30.2.4), the inputs (D), (I), (O) of Section 30.3 with Problems 30.3.1 and 30.3.3, Section 30.4, in particular Problems 30.4.6–30.4.8, and Section 30.5.

Section 30.4 of Chapter 30 observed that the Hecke algebra sees a Galois representation only through its traces. The Hecke algebra on the Eisenstein and cuspidal eigenspaces in Problem 31.1.5 has two components. In general the traces in a Hecke algebra need not be realized by a representation over that algebra. What structure do traces alone carry, and how do they measure Sha? The structure is a pseudocharacter; the ideal of products $b \cdot c$ of Chapter 30 can be read off from the traces; and the quotient by it carries extension classes, which bound the congruence from above by the length of a Selmer group. In the eigenform example, the cocycle obeys every linear relation among the matrices $U(g) - 1$ for the twist $U = \chi^{1-k}\rho_f$ (Problem 31.4.1). Theorem 31.4.1 realizes such cocycles by equivariant maps on submodules of families of matrices. Throughout, p is an odd prime.

31.1. Pseudocharacters of dimension two

Let G be a group and R a commutative ring in which 2 is invertible. A *pseudocharacter of dimension* 2 of G with values in R is a pair (T, D) of a function $T\colon G \to R$ and a homomorphism $D\colon G \to R^\times$ such that $T(1) = 2$ and, for all $g, h \in G$,

$$T(gh) = T(hg), \qquad T(gh) + D(g)\,T(g^{-1}h) = T(g)\,T(h).$$

By [Ch, Lemma 1.9] such pairs are the same as Chenevier's determinants of dimension 2. The function T is then a pseudocharacter of dimension 2 in the sense of Taylor [Ta, §1] and Rouquier [Ro], and conversely every such T arises in this way [Ch, Prop. 1.29]; see also [BC, §1.2]. The notion is due to Wiles in dimension two and to Taylor in general [BC, §1.1].

Problem 31.1.1. For every homomorphism $\rho\colon G \to \mathrm{GL}_2(R)$, $(\operatorname{tr}\rho, \det\rho)$ is a pseudocharacter. In particular, so is $(\psi_1+\psi_2, \psi_1\psi_2)$ for any two characters $\psi_1, \psi_2\colon G \to R^\times$.

Problem 31.1.2. If (T, D) is a pseudocharacter, then $D(g) = \frac{1}{2}\big(T(g)^2 - T(g^2)\big)$ and $T(g^{-1}) = D(g)^{-1}T(g)$ for all $g \in G$.

So D is determined by T, and we often write T for the pair.

Problem 31.1.3. Let $R \subseteq R_1 \times R_2$ be a subring in which 2 is invertible, and let (T_i, D_i) be pseudocharacters with values in R_i. If $(T_1(g), T_2(g)) \in R$ for every g, then $((T_1, T_2), (D_1, D_2))$ is a pseudocharacter with values in R.

Date: November 25, 2026.

The first example of a pseudocharacter that is not visibly a trace is the one carried by a Hecke algebra with one Eisenstein and one cuspidal point. Let G be profinite, let $\chi\colon G \to \mathbb{Z}_p^\times$ be a continuous character whose reduction $\bar\chi$ is not trivial, and let $\rho\colon G \to \mathrm{GL}_2(\mathbb{Q}_p)$ be a continuous representation with $\operatorname{tr}\rho(G) \subseteq \mathbb{Z}_p$, $\operatorname{tr}\rho \equiv 1+\chi \pmod p$ and $\operatorname{tr}\rho \neq 1+\chi$. Put

$$e := \min_{g\in G} v_p\big(\operatorname{tr}\rho(g) - 1 - \chi(g)\big), \qquad \mathcal{T}(g) := \big(1+\chi(g), \operatorname{tr}\rho(g)\big) \in \mathbb{Z}_p \times \mathbb{Z}_p.$$

Problem 31.1.4. The $\mathbb{Z}_p$-subalgebra of $\mathbb{Z}_p \times \mathbb{Z}_p$ generated by the $\mathcal{T}(g)$ is $\mathbf{T}_e := \{(u,v) : u \equiv v \pmod{p^e}\}$, and $x \mapsto (0,p^e)$ induces $\mathbb{Z}_p[x]/(x(x-p^e)) \cong \mathbf{T}_e$. The function $\mathcal{T}$ is a pseudocharacter with values in $\mathbf{T}_e$.

The ring $\mathbf{T}_e$ is the *toy Hecke algebra*: $x=0$ is the Eisenstein point, $x=p^e$ the cuspidal point, and e measures how close they are. It occurs in nature.

Problem 31.1.5. The $\mathbb{Z}_{691}$-subalgebra of $\mathrm{End}(M_{12}(\mathbb{Q}) \otimes \mathbb{Q}_{691})$ generated by the Hecke operators T_n, $n \geq 1$, on modular forms of weight 12 and level 1 is isomorphic to $\mathbb{Z}_{691}[x]/(x(x-691))$.

31.2. The reducibility ideal

Let R be a complete local noetherian ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}$ of characteristic $\neq 2$ (so $2 \in R^\times$), and let (T,D) be a pseudocharacter of G with values in R such that $T \equiv \chi_1 + \chi_2 \pmod{\mathfrak{m}}$ for two distinct characters $\chi_1, \chi_2\colon G \to \mathbb{F}^\times$. Fix $\sigma_0 \in G$ with $\chi_1(\sigma_0) \neq \chi_2(\sigma_0)$.

Problem 31.2.1. The polynomial $X^2 - T(\sigma_0)X + D(\sigma_0)$ has roots $\lambda_1, \lambda_2 \in R$ with $\lambda_i \equiv \chi_i(\sigma_0) \pmod{\mathfrak{m}}$, and $\lambda_1 - \lambda_2 \in R^\times$.

Define $a, d\colon G \to R$ by

$$a(g) := \frac{T(\sigma_0 g) - \lambda_2 T(g)}{\lambda_1 - \lambda_2}, \qquad d(g) := T(g) - a(g).$$

Problem 31.2.2. Suppose that $T = \operatorname{tr}\rho$ for $\rho\colon G \to \mathrm{GL}_2(R)$ with $\rho(\sigma_0) = \mathrm{diag}(\lambda_1,\lambda_2)$, and write $\rho = \left(\begin{smallmatrix} a' & b \\ c & d' \end{smallmatrix}\right)$. Then $a = a'$, $d = d'$, and $a(gh) - a(g)a(h) = b(g)c(h)$.

So a and d are the diagonal entries of a representation that need not exist, and the defect of a from being multiplicative stands in for the products $b(g)c(h)$.

Problem 31.2.3. $a \equiv \chi_1$ and $d \equiv \chi_2 \pmod{\mathfrak{m}}$. In particular $a(g) \in R^\times$.

Problem 31.2.4. $D(g) = a(g)T(g) - a(g^2)$ for every $g \in G$.

The *reducibility ideal* $I \subseteq R$ is the ideal generated by the elements $a(gh) - a(g)a(h)$, $g,h \in G$.

Problem 31.2.5. Modulo I, a and d are characters $G \to (R/I)^\times$, $T \equiv a + d$ and $D \equiv ad$.

Problem 31.2.6. Let $J \subsetneq R$ be an ideal, and let $\psi_1, \psi_2\colon G \to (R/J)^\times$ be characters with $\psi_i \equiv \chi_i \pmod{\mathfrak{m}}$ and $T \equiv \psi_1 + \psi_2 \pmod J$. Then $\psi_1 \equiv a$ and $\psi_2 \equiv d \pmod J$, and $I \subseteq J$.

Problems 31.2.5 and 31.2.6 prove the following; in particular I does not depend on σ_0. Over a henselian local ring in which $d!$ is invertible, Bellaïche and Chenevier give the corresponding reducibility ideal for each partition of the pairwise distinct, absolutely irreducible residual constituents of a d-dimensional pseudocharacter [BC, Prop. 1.5.1].

Theorem 31.2.1. *I is the smallest ideal J of R such that T is congruent modulo J to a sum of two characters lifting χ_1 and χ_2.*

For a representation ρ over a discrete valuation ring as in Section 30.2, Problems 31.2.2 and 30.4.6 give $I = \pi^{m+n}\mathcal{O}$, where $m+n$ is the length of the segment of stable lattices. Return to the toy Hecke algebra.

Problem 31.2.7. In Problem 31.1.4, suppose that ρ is irreducible, and let $m+n$ be the length of its segment of stable lattices (Problem 30.2.3, with $\chi_1 = 1$, $\chi_2 = \bar{\chi}$). Then $m+n \geq e$, and the reducibility ideal of $\mathcal{T}$ is $\{0\} \times p^{m+n}\mathbb{Z}_p = p^{m+n-e}\, x\mathbf{T}_e$.

The *Eisenstein ideal* of a pseudocharacter T with respect to two given characters $\psi_1, \psi_2 \colon G \to R^\times$ is the ideal I_{Eis} generated by the $T(g) - \psi_1(g) - \psi_2(g)$. By Theorem 31.2.1, $I \subseteq I_{\mathrm{Eis}}$ whenever the ψ_i lift the χ_i. In the setting of Chapter 30 the two ideals coincide.

Problem 31.2.8. Let k, p, f, λ be as in Section 30.3, and let $m+n$ be the length of the segment of stable lattices of ρ_f. Then

$$m+n = \min_{\ell \neq p} v\big(a_\ell(f) - 1 - \ell^{k-1}\big),$$

the minimum over primes $\ell \neq p$. So the reducibility ideal of $\operatorname{tr}\rho_f$ equals its Eisenstein ideal for $(1, \chi^{k-1})$.

For Δ and $p = 691$ both sides are 1 (Problem 30.4.8). When $K = \mathbb{Q}_p$, in the toy Hecke algebra built from $\rho = \rho_f$ and χ^{k-1} we get $e = m+n$, and the reducibility ideal is $x\mathbf{T}_e$: the Eisenstein component $\mathbf{T}_e/x\mathbf{T}_e = \mathbb{Z}_p$ is the largest quotient on which $\mathcal{T}$ is reducible.

31.3. The quotient by the reducibility ideal and Ext^1

Ribet's lemma produced a class modulo π. The reducibility ideal produces a class modulo I, which generates a copy of $\mathcal{O}/I$. Keep the notation of Section 30.2, with $\chi_1 \neq \chi_2$, and write ρ in the basis $\pi^m e_1, e_2$ of L_m as $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then the values of b generate $\mathcal{O}$, the values of c generate $I = \pi^{m+n}\mathcal{O}$, and by Problem 31.2.5 the reductions ψ_1, ψ_2 of a, d modulo I are characters. Put $\psi := \psi_1\psi_2^{-1}$.

Problem 31.3.1. $\kappa(g) := b(g)\, d(g)^{-1} \bmod I$ is a cocycle on G with values in $(\mathcal{O}/I)(\psi)$.

Problem 31.3.2. The $\mathcal{O}$-submodule of $H^1(G, (\mathcal{O}/I)(\psi))$ generated by the class of κ is isomorphic to $\mathcal{O}/I$.

Thus the quotient $\mathcal{O}/I$ embeds in a group of extensions of ψ_2 by ψ_1. For two distinct residual characters over a henselian local ring R, Bellaïche and Chenevier construct an injection from $\mathrm{Hom}_R(B, R/I)$ to the algebraic extension group of ψ_2 by ψ_1, where B is the upper right module of a chosen Cayley–Hamilton quotient [BC, Thm. 1.5.5]; for the continuous extension group under additional hypotheses, see [BC, Prop. 1.5.10(ii)]. Now take $G = G_{\mathbb{Q},p}$, and f, λ, $\mathcal{O}$ as in Problem 31.2.8,

so that $\psi \equiv \chi^{1-k} \pmod I$. As in Section 30.5, $\mathrm{Sha}_p(\mathbb{Q}, k-1) \otimes_{\mathbb{Z}_p} \mathcal{O}$ is the group of classes in $H^1(G_{\mathbb{Q},p}, (K/\mathcal{O})(1-k))$ that vanish on G_p. Use the coefficient embedding $(\mathcal{O}/I)(1-k) \hookrightarrow (K/\mathcal{O})(1-k)$, $\bar{a} \mapsto a/\pi^{m+n} + \mathcal{O}$.

Problem 31.3.3. The class of κ vanishes on G_p, and its image in $H^1(G_{\mathbb{Q},p}, (K/\mathcal{O})(1-k))$ generates a submodule isomorphic to $\mathcal{O}/I$. Hence $\mathrm{length}_{\mathcal{O}}\big(\mathrm{Sha}_p(\mathbb{Q}, k-1) \otimes \mathcal{O}\big) \geq m+n$.

This is the direction of Ribet and of Mazur and Wiles [MW], for one eigenform: a congruence of exponent $m+n$ produces a cyclic piece of Sha of that length. For Δ it gives length $\mathrm{Sha}_{691}(\mathbb{Q}, 11) \geq 1$, and Theorem 27.1.2 gives equality. Read the other way, Problem 31.3.3 bounds a congruence by a Selmer group: $m+n \leq \mathrm{length}_{\mathcal{O}}\big(\mathrm{Sha}_p(\mathbb{Q}, k-1) \otimes \mathcal{O}\big)$. In the proof, a Selmer length contributes, in this direction, to the upper bound for the cost of clearing a projection; this is the step of Chapter 65, *Denominators of projections to lifts*, that this chapter serves. In Problem 31.3.3 the class already lies in the kernel of restriction to G_p, so its full length contributes to the lower bound for Sha.

31.4. Cocycles that obey the relations

The proof works with cocycles obeying the simultaneous relations below, and Problem 31.4.1 gives an example. Let Λ be a commutative ring, G a group, X a finite set, and, for $i \in X$, let $U_i \colon G \to M_q(\Lambda)$ be homomorphisms of monoids; let $\varrho \colon G \to M_s(\Lambda)$ be another, and $\alpha \in \Lambda$. Put $\mathcal{N} := M_q(\Lambda)^X$, on which g acts by $(m_i)_i \mapsto (U_i(g)m_i)_i$, and $U(g) - 1 := (U_i(g) - 1)_i \in \mathcal{N}$. A map $\gamma \colon G \to (\Lambda/\alpha)^s$ is a *cocycle for* ϱ if $\gamma(gh) = \gamma(g) + \varrho(g)\gamma(h)$. It *obeys the relations among the* $U(g) - 1$ if, for every finitely supported $\theta \colon G \to \Lambda$,

$$\sum_g \theta(g)\,\big(U(g) - 1\big) = 0 \quad \Longrightarrow \quad \sum_g \theta(g)\,\gamma(g) = 0.$$

If all U_i are trivial, only $\gamma = 0$ obeys them.

Problem 31.4.1. In the setting of Problem 31.3.3, put $\Lambda := \mathcal{O}$, $\alpha := \pi^{m+n}$, $U := \chi^{1-k}\rho_f$ in the basis $\pi^m e_1, e_2$ of L_m (one representation, $q = 2$) and $\varrho := \chi^{1-k}$ ($s = 1$). Then $\kappa(g) = \chi(g)^{1-k} b(g) \bmod I$, and κ is a cocycle for ϱ that obeys the relations among the $U(g) - 1$.

From now on let γ be a cocycle for ϱ that obeys the relations among the $U(g) - 1$, and let $\mathcal{M} \subseteq \mathcal{N}$ be the Λ-span of the $U(g) - 1$, $g \in G$.

Problem 31.4.2. There is a unique Λ-linear map $\phi \colon \mathcal{M} \to (\Lambda/\alpha)^s$ with $\phi(U(g) - 1) = \gamma(g)$ for all g. The module $\mathcal{M}$ is stable under G, and $\phi(gy) = \varrho(g)\phi(y)$ for $y \in \mathcal{M}$.

So the graph of ϕ is a G-stable submodule of $\mathcal{N} \times (\Lambda/\alpha)^s$, with g acting on the second factor through ϱ, on which the first projection is injective. It is usually too small: even over $\mathbb{Z}_p$, $\mathcal{M}$ need not contain $p^j\mathcal{N}$ for any $j \geq 0$. Let Λ be noetherian. By the Artin–Rees lemma [AM, Cor. 10.10], applied to the submodule $\mathcal{M}$ of the finitely generated module $\mathcal{N}$, there is $\nu \geq 1$ with $\mathcal{M} \cap \alpha^\nu \mathcal{N} \subseteq \alpha\mathcal{M}$.

Problem 31.4.3. Let $\mathcal{M} \cap \alpha^\nu \mathcal{N} \subseteq \alpha\mathcal{M}$. Then

$$Y := \big\{ \big(y + \alpha^\nu v,\ \phi(y)\big) : y \in \mathcal{M},\ v \in \mathcal{N} \big\}$$

is a G-stable submodule of $\mathcal{N} \times (\Lambda/\alpha)^s$, the first projection is injective on Y, and $\big(U(g) - 1 + \alpha^\nu v, \gamma(g)\big) \in Y$ for all $g \in G$ and $v \in \mathcal{N}$.

Problem 31.4.4. Let $\Lambda = \mathbb{Z}_p$, $\alpha = p$, $G = \mathbb{Z}$, X a point, $U(j) = \left(\begin{smallmatrix} 1 & jp \\ 0 & 1 \end{smallmatrix}\right)$, $\varrho = 1$ and $\gamma(j) = j \bmod p$. Then γ obeys the relations among the $U(j) - 1$, and the least ν with $\mathcal{M} \cap p^\nu M_2(\mathbb{Z}_p) \subseteq p\mathcal{M}$ is $\nu = 2$. For $\nu = 1$ the set Y of Problem 31.4.3 contains $(0, 0)$ and $(0, 1)$.

Problems 31.4.2 and 31.4.3 prove the following theorem, which is stated as in the proof.

Theorem 31.4.1. *Let Λ be a commutative noetherian ring, $\alpha \in \Lambda$, G a group, X a finite set, and $U_i \colon G \to M_q(\Lambda)$, $i \in X$, and $\varrho \colon G \to M_s(\Lambda)$ homomorphisms of monoids. Let $\gamma \colon G \to (\Lambda/\alpha)^s$ be a cocycle for ϱ that obeys the relations among the $U(g) - 1$. Then there are $\nu \geq 0$ and a G-stable Λ-submodule Y of $M_q(\Lambda)^X \times (\Lambda/\alpha)^s$, with g acting by $\big((m_i)_i, w\big) \mapsto \big((U_i(g)m_i)_i, \varrho(g)w\big)$, such that the first projection is injective on Y and $\big((U_i(g) - 1)_i + \alpha^\nu v, \gamma(g)\big) \in Y$ for all $g \in G$ and all $v \in M_q(\Lambda)^X$.*

If Λ is a discrete valuation ring and $\alpha \neq 0$, the first projection identifies Y with a lattice in $M_q(\Lambda)^X$: its image contains $\alpha^\nu M_q(\Lambda)^X$.
In the Lean formalization. In the Lean proof [GL], Theorem 31.4.1 is `ribetCocycles.exists_graph_subrepresen` and the cocycles that obey the relations form `ribetCocycles`, both in `New/Congruences/LocalLoss/Basic.lean` of the readable edition.

Hints

§31.1.

31.1.1: Cayley–Hamilton: $\rho(g) + \det \rho(g)\, \rho(g)^{-1} = \operatorname{tr} \rho(g)$.
31.1.2: Take $h = g$, then $h = 1$.
31.1.3: Problem 31.1.2.
31.1.4: Subtract the scalar $1 + \chi(g)$ from $\mathcal{T}(g)$. Then Problems 31.1.2, 31.1.1 and 31.1.3.
31.1.5: Use the eigenbasis E_{12}, Δ, Problem 30.1.1, and $\tau(2) = -24$.

§31.2.

31.2.1: Hensel's lemma.
31.2.2: Compute $\operatorname{tr}(\rho(\sigma_0)\rho(g))$.
31.2.3: Reduce modulo $\mathfrak{m}$ and use $T(\sigma_0 g) \equiv \chi_1(\sigma_0 g) + \chi_2(\sigma_0 g)$.
31.2.4: Express $T(\sigma_0 g^2)$ by the defining identity with $(g, g\sigma_0)$, and $T(g^2)$ by Problem 31.1.2.
31.2.5: Problems 31.2.3 and 31.2.4.
31.2.6: Problem 31.1.2, and the polynomial of Problem 31.2.1 modulo J.
31.2.7: First, the reduction of a stable lattice has semisimplification $1 \oplus \bar{\chi}$: its trace is $1 + \bar{\chi}$, its determinant is $\bar{\chi}$ by Problem 31.1.2, and Brauer–Nesbitt applies. The roots of Problem 31.2.1 and the function a may be computed in each factor. Use Problem 31.2.2 in the second factor, and note that $\mathbf{T}_e$ projects onto the second factor.
31.2.8: One inequality is Problem 30.4.7. For the other, apply Problem 31.2.6 with J the ideal generated by the $a_\ell(f) - 1 - \ell^{k-1}$, and Chebotarev.

§31.3.

31.3.1: Modulo I the matrix is upper triangular; multiply two of them.

31.3.2: Evaluate at σ_0.

31.3.3: Run Problem 30.3.3 modulo I, as in Problem 30.4.7; $(\mathcal{O}/I)(1-k)$ has no invariants under I_p. Then Problem 27.1.1.

§31.4.

31.4.1: Problem 30.4.7, and the upper right entry of $U(g)$.

31.4.2: Expand $U(gh)-1$ by the cocycle rule.

31.4.3: For injectivity, α kills $(\Lambda/\alpha)^s$.

31.4.4: Compute $\mathcal{M}$ first.

References

[AM] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[BC] J. Bellaïche and G. Chenevier, *Families of Galois representations and Selmer groups*, Astérisque **324** (2009).

[Ch] G. Chenevier, *The p-adic analytic space of pseudocharacters of a profinite group and pseudorepresentations over arbitrary rings*, in: Automorphic Forms and Galois Representations, Vol. 1, London Math. Soc. Lecture Note Ser. 414, Cambridge Univ. Press, 2014, 221–285; `https://arxiv.org/abs/0809.0415`.

[GL] L. Sernau, *GRH for Dirichlet L-functions, in Lean 4*, a shorter rewriting of the Lean proof, text by Claude, `https://github.com/lsernau/grh-lean`, commit `72fead1`, readable edition `grh/`.

[MW] B. Mazur and A. Wiles, *Class fields of abelian extensions of* $\mathbf{Q}$, Invent. Math. **76** (1984), 179–330.

[Ro] R. Rouquier, *Caractérisation des caractères et pseudo-caractères*, J. Algebra **180** (1996), 571–586.

[Ta] R. Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991), 281–332.